K19U 0185

Reg. No. : .....

Name : .....

VI Semester B.C.A. Degree (CBCSS – Reg./Supple./Improv.) Examination, April 2019
(2014 Admission Onwards)
CORE COURSE (Elective)
6B19BCA – E01 : Information Security

Time : 3 Hours Max. Marks : 40

SECTION – A

1. **One** word questions. **(8×0.5=4)**
   a) In computer security, _____ means that computer system assets can be modified only by authorized parities.
   b) _____ is a program that can modify other programs by a copy of the virus program, which can go on to infect other programs.
   c) _____ changes the location of the symbols, instead of substituting one symbol for another.
   d) We can combine the additive and multiplicative ciphers to get _____
   e) What is the preprocess step before key expansion in a compression ?
   f) _____ refers to the situation in which two or more different keys can create the same ciphertext from the same plaintext.
   g) OAEP stands for _____
   h) _____ and _____ are the two keys used for asymmetric encryption.

SECTION – B

Write short notes on **any seven** of the following questions. **(7×2=14)**

2. Define the term Virus.
3. Write short note on integrity.

P.T.O.

4. Discuss stream ciphers, in brief.
5. Explain vigenere cipher.
6. List and explain the objectives of information security.
7. Explain any two design criteria of DES.
8. What is the factoring problem in RSA ?
9. Write short note on timing attack.
10. What is message authentication ?
11. Describe different attacks on digital signature.

SECTION – C

Answer **any four** of the following questions. **(4×3=12)**

12. Write short on Steganography.
13. Explain different substitution ciphers.
14. Explain different types of DES function.
15. Differentiate between linear and differential cryptanalysis.
16. Explain the key generation process in RSA algorithm.
17. List the various security services provided by digital signature.

SECTION – D

Write an essay on **any two** of the following questions. **(2×5=10)**

18. Explain digital signature schemes.
19. Discuss the two broad categories of traditional symmetric key ciphers with focus on different cipher cryptanalysis.
20. Explain the structure of DES.
21. Explain the computational aspects of RSA algorithm.